Office of the Auditor General

Follow-Up Report on Prior Audit Recommendations

Statewide Oracle Database Controls

Department of Technology, Management, and Budget

May 2018

State of Michigan Auditor General

Doug A. Ringler, CPA, CIA

071-0565-14F

The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof.

Article IV, Section 53 of the Michigan Constitution

OAG
Office of the Auditor General

Report Summary

Follow-Up Report

Statewide Oracle Database Controls

Department of Technology, Management, and Budget (DTMB)

Report Number:
071-0565-14F

Released:
May 2018

We conducted this follow-up to determine whether DTMB had taken appropriate corrective measures in response to the two material conditions noted in our March 2015 audit report.

Prior Audit Information
Finding #1 - Material condition More comprehensive security configurations vital to protect databases. Agency agreed.
Finding #3 - Material condition Formal training program could improve database administrators' database management. Agency agreed.

Follow-Up Results		
Conclusion	**Finding**	**Agency Preliminary Response**
Partially complied	Reportable condition exists. See Finding #1.	Partially agrees
Complied	Not applicable	

Obtain Audit Reports

Online: audgen.michigan.gov

Phone: (517) 334-8050

Office of the Auditor General
201 N. Washington Square, Sixth Floor
Lansing, Michigan 48913

Doug A. Ringler, CPA, CIA
Auditor General

Laura J. Hirst, CPA
Deputy Auditor General

This Page Left Intentionally Blank

OAG
Office of the Auditor General

Doug A. Ringler, CPA, CIA
Auditor General

201 N. Washington Square, Sixth Floor • Lansing, Michigan 48913 • Phone: (517) 334-8050 • audgen.michigan.gov

May 15, 2018

Mr. David L. DeVries
Director, Department of Technology, Management, and Budget
Chief Information Officer, State of Michigan
Lewis Cass Building
Lansing, Michigan

Dear Mr. DeVries:

This is our follow-up report on the two material conditions (Findings #1 and #3) and two corresponding recommendations reported in the performance audit of Statewide Oracle Database Controls, Department of Technology, Management, and Budget. That audit report was issued and distributed in March 2015. Additional copies are available on request or at audgen.michigan.gov.

Your agency provided the preliminary response to the follow-up recommendation included in this report. The *Michigan Compiled Laws* and administrative procedures require an audited agency to develop a plan to comply with the recommendations and to submit it within 60 days of the date above to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

We appreciate the courtesy and cooperation extended to us during our follow-up. If you have any questions, please call me or Laura J. Hirst, CPA, Deputy Auditor General.

Sincerely,

Doug Ringler

Doug Ringler
Auditor General

This Page Left Intentionally Blank

TABLE OF CONTENTS

STATEWIDE ORACLE DATABASE CONTROLS

INTRODUCTION, PURPOSE OF FOLLOW-UP, AND DESCRIPTION

INTRODUCTION

This report contains the results of our follow-up of the two material conditions* (Findings #1 and #3) and two corresponding recommendations reported in our performance audit* of Statewide Oracle Database Controls, Department of Technology, Management, and Budget (DTMB), issued in March 2015.

PURPOSE OF FOLLOW-UP

To determine whether DTMB had taken appropriate corrective measures to address our corresponding recommendations.

DESCRIPTION

A database is a collection of information organized so that it can be easily accessed, managed, and updated. A database management system (DBMS), such as Oracle Database, is a software system that uses a standard method of cataloging, retrieving, and running queries on data. A DBMS manages input data, organizes data, and provides ways for the data to be modified or extracted by users or other programs.

The State maintains approximately 575 Oracle databases that are used for transaction processing and reporting by the State's various IT systems. Some of these databases contain confidential information and are classified as critical to State operations.

** See glossary at end of report for definition.*

PRIOR AUDIT FINDINGS AND RECOMMENDATIONS; AGENCY PLAN TO COMPLY; AND FOLLOW-UP CONCLUSIONS, RECOMMENDATION, AND AGENCY RESPONSE

FINDING #1

Audit Finding Classification: Material condition.

Summary of the March 2015 Finding:
DTMB did not fully establish and implement effective security configurations* for the State's Oracle databases to help prevent or detect inappropriate access to or modification of the State's data.

Recommendation Reported in March 2015:
We recommended that DTMB fully establish and implement effective security configurations for the State's Oracle databases.

AGENCY PLAN TO COMPLY*

DTMB's plan to comply dated August 14, 2015 indicated that it had established a Database Security Standards Committee (DSSC) in June 2013 and had published security standards and procedures in June 2014 related to Oracle database security and data classification. Also, DTMB indicated that it would update Oracle database security standards and publish the revised version by September 30, 2015.

DTMB's plan to comply also indicated that it had established a Database Security Program and implemented database encryption in June 2014, would install Oracle database security program software by October 1, 2015, and would configure and tailor deployment of each Oracle database security product to produce the maximum security protection for State of Michigan (SOM) agencies by May 1, 2016. Any agency that had not completed configuration and deployment implementation by this date would require an approved exception request to extend its completion date.

FOLLOW-UP CONCLUSION

Partially complied. A reportable condition* exists.

We assessed the security configurations for 6 of the State's Oracle databases, including 5 production databases and 1 nonproduction database. Our follow-up noted:

a. DTMB published updated standards related to Oracle database security configurations which resulted in additional compliance with industry best practice recommendations. However, some potentially vulnerable security configurations existed on 6 (100%) of the 6 databases reviewed. Because of the confidentiality of

** See glossary at end of report for definition.*

these configurations, we summarized our testing results for presentation in this portion of the finding and provided the detailed results to DTMB management.

b. DTMB improved its communication of security requirements and its monitoring of security settings for databases managed by vendors. DTMB's vendor contracts include language that requires vendors to adhere to State security standards. Updates to these standards are communicated to the vendors.

   However, DTMB did not sufficiently monitor the security settings of two databases managed by third-party vendors. One of the two databases was not actively monitored by DTMB. The other database was actively monitored; however, not all security settings were assessed.

FOLLOW-UP RECOMMENDATION

We recommend that DTMB continue to establish and implement effective security configurations for the State's Oracle databases and monitor vendors to ensure compliance with industry best practices and State standards.

FOLLOW-UP AGENCY RESPONSE

DTMB provided us with the following response:

DTMB partially agrees with the recommendation. DTMB continues to refine and expand security configurations established over the State's Oracle databases.

The DTMB published standards are reviewed annually for alignment and re-alignment to the Center for Internet Security benchmarks and Michigan Cyber Security. The 2018 updates are expected to address the non-compliances reported through this audit's compliance testing.

DTMB Enterprise Oracle Database Security Program (EODSP) has already successfully implemented database encryption and database audit logging features for databases not on the decommission/exception list, as of February 2018. This program is also tracking progress on implementing additional database security features and tools and the few remaining Next Generation Digital Infrastructure (NGDI) migrations.

DTMB intends to leverage the newly implemented Tenable software for security scanning and to ensure all State of Michigan databases are compliant with Database Security Standards 1340.00.60.02 and 1340.00.60.02.01.

FINDING #3

Audit Finding Classification: Material condition.

Summary of the March 2015 Finding:
DTMB did not establish a formal training program or take other necessary action to ensure that all database administrators* (DBAs) received sufficient training.

Recommendation Reported in March 2015:
We recommended that DTMB establish a formal training program or take other steps to ensure that all DBAs managing the State's Oracle databases receive sufficient training.

AGENCY PLAN TO COMPLY

DTMB's plan to comply dated August 14, 2015 indicated it had conducted a training needs analysis to identify gaps in employee training and related training needs. DTMB indicated that it would provide each SOM agency with training options and recommendations to ensure that DBAs achieve an appropriate level of Oracle security competency and maintain and enhance the DBAs' knowledge of product improvements, proactive problem mitigation, and best practices by September 30, 2015. DTMB also indicated that each SOM agency would be required to fund and plan the DBA training and that an exception would be required for any SOM agency that did not have a DBA training program completed and funded by December 31, 2015.

FOLLOW-UP CONCLUSION

Complied.

DTMB assessed the training needs of the DBAs and established a DBA training program. Survey responses of 22 DBAs participating in the program generally indicated that a sufficient level of training was provided. Specifically:

a. Twenty-one (95%) of the 22 DBAs indicated that they had received training on all or some of the versions of Oracle database that they are managing.

b. Twenty (91%) of the 22 DBAs indicated that DTMB had provided them with a sufficient level of training to appropriately configure and maintain an adequately secured Oracle database environment.

c. Nineteen (86%) of the 22 DBAs indicated that they had received sufficient training to perform their job effectively in all areas.

** See glossary at end of report for definition.*

FOLLOW-UP METHODOLOGY, PERIOD, AND AGENCY RESPONSES

METHODOLOGY

We reviewed DTMB's corrective action plan; policies, standards, and procedures; and industry best practices relating to Oracle database security. Specifically, for:

a. Finding #1, we:

- Interviewed DTMB to obtain an understanding of the security configurations implemented for Oracle databases and the processes in place to monitor the vendors that manage the State's Oracle databases.
- Judgmentally selected 5 production databases and 1 nonproduction database and tested their configurations against industry best practices and State standards.
- Reviewed contract requirements and security configuration compliance reports for the Oracle databases managed by vendors.

b. Finding #3, we:

- Reviewed DTMB's Oracle database training program and training attendance records.
- Surveyed 29 Oracle DBAs and evaluated the 22 responses received to assess the sufficiency of the training provided.
- Reviewed a random sample of individual performance management plans for 4 DBAs to determine whether their training needs had been assessed and whether the training was evaluated for effectiveness.

PERIOD

Our follow-up generally covered April 1, 2017 through March 31, 2018.

AGENCY RESPONSES

Our follow-up report contains 1 recommendation. DTMB's preliminary response indicates that it partially agrees with the recommendation.

The agency preliminary response that follows the follow-up recommendation in our report was taken from the agency's written comments and oral discussion at the end of our fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require an audited agency to develop a plan to comply with the recommendations and to submit it within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

GLOSSARY OF ABBREVIATIONS AND TERMS

agency plan to comply

The response required by Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100). The audited agency is required to develop a plan to comply with Office of the Auditor General audit recommendations and to submit the plan within 60 days after release of the audit report to the Office of Internal Audit Services, State Budget Office. Within 30 days of receipt, the Office of Internal Audit Services is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

configuration

The way a system is set up. Configuration can refer to either hardware or software or the combination of both.

database

A collection of information that is organized so that is can be easily accessed, managed, and updated.

database administrator (DBA)

The person responsible for both the design of the database, including the structure and contents, and the access capabilities of application programs and users of the database. Additional responsibilities include operation, performance, integrity, and security of the database.

DBMS

database management system.

DTMB

Department of Technology, Management, and Budget.

IT

information technology.

material condition

A matter that, in the auditor's judgment, is more severe than a reportable condition and could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program.

performance audit

An audit that provides findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria. Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program performance and operations, reduce costs, facilitate decision-making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability.

reportable condition

A matter that, in the auditor's judgment, is less severe than a material condition and falls within any of the following categories: an opportunity for improvement within the context of the audit objectives; a deficiency in internal control that is significant within the context of the audit objectives; all instances of fraud; illegal acts unless they are inconsequential within the context of the audit objectives; significant violations of provisions of contracts or grant agreements; and significant abuse that has occurred or is likely to have occurred.

SOM

State of Michigan.

This Page Left Intentionally Blank

OAG

Office of the Auditor General

Independent Objective Transparent

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud
Hotline: (517) 334-8060, Ext. 1650